Simple Saml Php su Apache/Debian How-To

Preparare Apache e PHP opportunamente.

Installare il modulo php5-mcrypt.

Una volta installato simplesamlphp e' possibile verificare via web la corretta configurazione sull'apposita pagina “Controllo dell'installazione di PHP”

Aumentare la dimensione ammissibile degli header se si usa la suhosin patch su Apache.

```
echo "suhosin.get.max_value_length = 2048" >
/etc/php5/conf.d/suhosin.simplasaml.ini
/etc/init.d/apache2 restart
```

Download Simple Saml PHP

```
wget http://simplesamlphp.googlecode.com/files/simplesamlphp-1.10.0.tar.gz
```

Decompress

```
tar xzf simplesamlphp-1.10.0.tar.gz
```

Link

```
ln -s simplesamlphp-1.10.0 simplesamlphp
```

```
cd simplesamlphp
cd conf
```

Modificare il file config.php personalizzando

```
'auth.adminpassword'        => 'setnewpasswordhere',
```

Valorizzare

```
'secretsalt' => 'y65znz4u1mzcfxz7htjfl4zzzgtvgyuc',
```

con l-output del comando:

```
tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32
count=1 2>/dev/null;echo
```

```
'technicalcontact_name'     => 'Daniele Albrizio',
'technicalcontact_email'    => 'idem@units.it',
'language.default'      => 'no',
'timezone' => 'Europe/Rome',
```

Creiamo un certificato da poi condividere con l'IdP o con la Federazione per firmare i metadati:

```
cd simplesamlphp/cert
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out saml.crt -
keyout saml.pem
  Country Name (2 letter code) [AU]:IT
  Organization Name (eg, company) [Internet Widgits Pty Ltd]:University of
Trieste
  Common Name (eg, YOUR name) []:netstart.units.it
  Email Address []:rete@units.it
```

Nel file *authsources.php* valorizzare il campo idp per il default-sp

```
      // An authentication source which can authenticate against both SAML
2.0
      // and Shibboleth 1.3 IdPs.
      'default-sp' => array(
              'saml:SP',
              // The entity ID of this SP.
              // Can be NULL/unset, in which case an entity ID is generated
based on the metadata URL.
              'entityID' => NULL,
              // The entity ID of the IdP this should SP should contact.
              // Can be NULL/unset, in which case the user will be shown a
list of available IdPs.
              //'idp' => NULL,
              'idp' => "https://idemfero.units.it/idp/shibboleth",
              // The URL to the discovery service.
              // Can be NULL/unset, in which case a builtin discovery
service will be used.
              'discoURL' => NULL,
             // Encrypt Assertions
             'privatekey' => 'saml.pem',
             'certificate' => 'saml.crt',
      ),
```

Exchange metadata with the IdP

Scaricate i metadata dell'IdP nell-SP

```
cd /tmp
wget https://idemfero.units.it/idp/shibboleth -O idemfero-metadata.xml
```

Andare sul sito dell'SP con un browser alla pagina https://.../simplesaml/admin/metadata-converter.php (Federazione → Convertitore di metadati dal formato XML al formato simpleSAMLphp) e incollare il contenuto del file idemfero-metadata.xml

Copiare il risultato della finestra con nome saml20-idp-remote.php **sovrascrivendo** il corrispondente

file in *simplesamlphp/metadata/saml20-idp-remote.php* **cancellando** i dati degli altri IdP contenuti nel file, ma ricordandosi di aprire il tag "*<?php*" ad inizio file.

E' possibile verificarne il corretto caricamento nella sezione *Metadati SAML 2.0 IdP (Trusted)* della pagina *Federazione*.

Caricare i metadata dell'SP nell'IdP

Andate sulla pagina "Federazione" di simplesamlphp dopo essere entrati come amministratori. Alla voce "Metadati SAML 2.0 SP" cliccare su *Mostra metadati*

Copiare i metadati SAML 2 risultanti e spedirli ad idem@units.it perché siano messi nella directory dei metadati dell'Identity Provider.

Testare il funzionamento dell'SP

Autenticazione → Prova le fonti di autenticazione configurate → default-sp